REMARKS

This response is submitted along with a request for a three month extension, a Petition for Revival and appropriate fees in reply to the Office Action dated July 17, 2006. The present application went abandoned on January 17, 2007 for failure to respond to the Office Action of July 17, 2006. However, Applicants respectfully submit that the delay in responding to the Office Action was unintentional. Accordingly, Applicants respectfully request revival of the present application in accordance with the Petition for Revival provided herewith.

Claims 1-14 are pending in the present application. The Official Action allows Claims 1-3 and 6. Claims 10 and 11 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Claims 8 and 9 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Claims 4, 5, 7, and 14 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,870,474 to Anthony J. Wasilewski, et al. Applicant appreciates Examiner's allowance of Claims 1-3 and 6. As described below, Applicant has amended Claims 4, 8, 9, and 10 to overcome the rejections. Claim 5 has been cancelled. Further as described below, Applicant respectfully traverses the rejection of Claim 11. Based on the foregoing amendments and the following remarks, Applicant respectfully requests reconsideration of the present application and allowance of the amended set of claims.

1. The Present Application

As described by the application, a technique is provided for broadcasting secure messages to a plurality of receiving nodes. For example, secure messages may be wirelessly transmitted to each of a plurality of wireless subscribers. The secure messages include data that has been encrypted with a key. The encrypted data and a hashed representation of the key may then be combined into a broadcast message that is transmitted to each of the receiving nodes. In this regard, it is noted that the same broadcast message containing the same encrypted data and the same hashed key, is transmitted to each of the intended recipients.

Upon receiving the broadcast message, each receiving node can parse the broadcast message to separately identify the encrypted data and the hashed key. Each receiving node may also include a plurality of keys that have been prestored in memory, that is, stored by the receiving node prior to receipt of the broadcast message. The receiving node then precedes to

hash the plurality of prestored keys. The hashed representations of the prestored keys may be compared to the hashed key included in a broadcast message to determine if a match exists. If a match exists, the encrypted data can be decrypted utilizing the key that has a hash that matches the hashed key included in the broadcast message. If no match exists, the receiving node can request a key from a network entity and, upon receipt of the additional key, can create a hash of the additional key and then compare the hashed representation of the additional key to the hashed key received in the broadcast message to determine if the additional key provided by the network entity matches that with which the data has been encrypted. If a match is found, the encrypted data is decrypted utilizing the additional key.

By permitting encrypted data to be decrypted by means of a prestored key, the messages may be transmitted with increased security since the key need not be transmitted in a manner that can be deciphered by an unintended recipient. By including a hashed representation of the key in the broadcast message, however, the receiving node can readily determine the key that was used to encrypt the data such that the data may be properly decrypted. Moreover, by utilizing the same key to encrypt the data for each of a plurality of receiving nodes, the same message may be broadcast to and decrypted by each of the intended recipients, thereby conserving network bandwidth and reducing the processing requirements on the transmission side of the network. It is noted that the conservation of bandwidth is of particular concern in instances in which the messages are being wireless transmitted to a plurality of wireless receiving nodes since the wireless network that supports the transmission may have only a limited bandwidth that can be devoted to the transmission of the messages.

As noted, the method of embodiments of the claimed invention is designed to broadcast a secure message to a plurality of receiving nodes, typically while conserving the bandwidth required for the broadcast of the secure message. For various reasons, it is sometimes desirable to prevent one or more of the nodes that previously received and decrypted the secure messages from being capable of decrypting similarly encrypted messages in the future. As described by the application, for example, the receiving nodes may have subscribed to a news service and been provided with the key(s) necessary to decrypt the encrypted news stories that are broadcast to the receiving nodes. Upon the expiration of a node's subscription, however, the receiving node whose subscription has expired should be prevented from decrypting similarly encrypted

news stories that are broadcast in the future, while not altering the capability of the other receiving nodes to receive and decrypt any future news stories. In this regard, a message including a NULL key may be transmitted to the node that is desired to be removed from the plurality of receiving nodes. In response to this message, the node to which the NULL key is transmitted replaces the pre-stored keys with the NULL key such that the respective node is thereafter unable to decrypt a broadcast message in the same manner as before. By being capable of transmitting a message containing a NULL key to the node to be removed without having to retransmit the list of keys to all of the remaining receiving nodes, the bandwidth utilized to administer the broadcast network is further conserved.

2. The Wasilewski '474 Patent

The Wasilewski '474 patent describes a method and apparatus for securely transmitting programs, such as video, audio and data, between a service provider and a customer's set top unit over a broadband digital network. In order to transmit a program, the Wasilewski method and apparatus initially encrypts a program with a first key, such as a random number generated key. The first key is then encrypted with a second key, termed a multisession key (MSK), that is also a randomly generated key. This second key is then encrypted utilizing the public key of the customer's set top unit to which the program is directed. The encrypted program, the encrypted first key and the encrypted second key are then transmitted to the set top unit.

The Wasilewski '474 patent also describes a message authentication code (MAC) and an entitlement management message (EMM) being sent to the set top unit for authentication purposes. In order to generate the MAC and the EMM, hashed representations are created as described below. In one context, control words are delivered to a set top unit along with a message authentication code (MAC). As described in column 9 of the Wasilewski '474 patent, the non-encrypted control word, other data and the MSK are concatenated together and then hashed to produce a MAC. The MAC is appended to an encrypted form of the control word (encrypted with the MSK) and then transmitted to the set top unit along with the resulting hash value. By reversing the process, the message may be authenticated.

The EMM including the MSK may also be transmitted such that the set top unit can confirm that an authorized source transmitted the program and the associated encryption keys.

The EMM is hashed and the resulting hash value is encrypted using the private key of the service provider that is to transmit the program content. This encryption process creates a digital signature token that is appended to the EMM. The digitally-signed EMM is then encrypted with the public key of the set top unit that is to receive the message. The signed, encrypted EMM may then also be transmitted to the set top unit.

Upon receipt, the set top unit can decrypt the signed, encrypted EMM with its private key to produce the EMM that includes the MSK and the digital signature token. The token is then decrypted with the public key of the service provider to result in a hashed representation of the EMM. The EMM that was provided along with the digital signature token is then hashed and the two hashed representations are compared. If equivalent and if the MAC was properly authenticated, the decryption process may continue. In this regard, the decryption of the program may commence by initially decrypting the encrypted second key, i.e., the encrypted MSK, utilizing the private key of the set top unit. The resulting second key is then compared to the MSK that was recovered from the EMM. If the MSKs match, the MSK is considered to be authenticated and the decryption process continues. If the MSKs differ, however, the authenticity of the encrypted program may be in question. If the MSK is authenticated, the encrypted first key may then be decrypted utilizing the MSK. The resulting first key may then be utilized to decrypt the program such that the set top unit can thereafter display the program.

3. Amended Independent Claim 10 is Patentable

Claim 10 has been amended and is now directed to a computer program product instead of an electromagnetic data signal and as such is statutory subject matter under 35 U.S.C. § 101. As such, the rejection under 35 U.S.C. § 101 is overcome. Since amended independent Claim 10 is directed toward statutory subject matter and the Examiner found arguments distinguishing Claim 10 from Wasilewski in the response to the Office Action of October 31, 2005 persuasive (Page 2 of Office Action of July 17, 2006), Applicant respectfully submits that amended independent Claim 10 is in condition for allowance.

4. Claims 11 and 12 are Patentable

Applicant respectfully traverses the rejection of independent Claim 11 as being directed to non-statutory subject matter under 35 U.S.C. § 101. Claim 11 is directed to a computer program product. The Office Action states that "there is no recitation of a limitation directed towards a computer-readable memory medium that stores the instruction set" (Page 4 of Office Action of July 17, 2006). However, independent Claim 11 includes the recitation of "a tangible medium that stores the computer readable code." As such, Claim 11 does include a recitation directed toward a computer-readable memory medium that stores the instruction set and Applicant therefore respectfully submits that the rejection is overcome. Since Claim 11 is directed toward statutory subject matter and the Examiner found amendments and arguments patentably distinguishing Claim 11 from Wasilewski in the response to the Office Action of October 31, 2005 persuasive (Page 2 of Office Action of July 17, 2006), Applicant respectfully submits that independent Claim 11 is in condition for allowance. Applicant further respectfully submits that Claim 12 is in condition for allowance for at least the foregoing reasons since Claim 12 includes all of the recitations of independent Claim 11.

5. Amended Independent Claims 8 and 9 and Their Dependent Claims are Patentable

Applicant has amended independent Claims 8 and 9 by directing the claims to a computer-readable memory having computer-readable program code portions stored therein so as to overcome the 35 U.S.C. § 112, second paragraph rejection for being indefinite. Applicant respectfully submits that the rejection of independent Claims 8 and 9 is therefore overcome. As such, since the Office Action states that "Claims 8 and 9 would be allowable if rewritten or amended to overcome the rejection," (Page 7 of the Office Action of July 17, 2006) applicant respectfully submits that Claims 8 and 9 are in condition for allowance. Since dependent Claim 13 includes all of the recitations of Claim 9 and has been amended to reflect the amendment to Claim 9, applicant also respectfully submits that Claim 13 is in condition for allowance for at least the reasons stated above.

6. Independent Claim 4 and its Dependent Claims are Patentable

Although Applicant respectfully disagrees that Wasilewski anticipates independent Claim 4 for the reasons argued in the previous response, Applicant has amended the claim to include

the recitation requesting a key from a network entity if no prestored key is found to have a hash that matches said received hashed key so as to further patentably distinguish over Wasilewski. As such, amended independent Claim 4 is directed to a method for decrypting a message received over a broadcast network that includes the steps of: (i) receiving data comprising an encrypted message and a hashed key at a node in the broadcast network, (ii) parsing the data to derive the encrypted message and the hashed key, (iii) comparing the received hashed key with a plurality of keys that are prestored at the node and selecting a key having a hash that matches the received hashed key, (iv) decrypting the encrypted message with the matching key if a match was found, and (v) requesting a key from a network entity if no prestored key is found to have a hash that matches the received hashed key.

In contrast to independent Claim 4, the Wasilewski '474 patent neither teaches nor suggests requesting a key from a network entity if no prestored key is found to have a hash that matches said received hashed key. In reference to now cancelled Claim 5, which previously included the recitation now added by amendment to Claim 4, the Official Action contends that the Wasilewski '474 patent does request a key from the network entity if a matching key is not found by pointing to column 11, line 48-50. With reference to the internal list of public keys of the authorized service providers that is maintained by the set top unit and was described above, column 11, line 48-50 states "[t]his information is provided to the STU [set top unit] **90** by the conditional access authority to ensure the integrity of the public keys." While the conditional access authority does provide the public keys of the authorized service providers to the set top unit, the Wasilewski '474 patent does not teach or suggest that the conditional access authority provides these public keys in response to a request from the set top unit, let alone a request from the set top unit that is generated in response to having not found any key that matches the hashed key received along with the encrypted message as set forth by independent Claim 4. In addition, the cited reference neither teaches nor suggests sending a request for a key to a network entity if no matching key was found as set forth by independent Claim 9 and, in fact, Wasilewski is not cited for any such disclosure. Moreover, amended Claim 4 now includes substantially the same recitations as Claim 9, which the Examiner stated would be allowable if amended to overcome the 35 U.S.C. § 112, second paragraph rejection (Page 7 of the Office Action of July 17, 2006). As such, Applicant also submits that independent Claim 4 is not taught or suggested by the cited

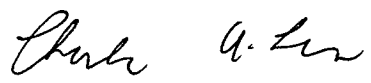
reference such that the rejection of Claim 4, as well as Claims 7 and 14 that depend there from, is overcome.

CONCLUSION

In view of the amended claims and the remarks presented above, it is respectfully submitted that all of the claims of the present application are in condition for immediate allowance. It is therefore respectfully requested that a notice of allowance be issued. The Examiner is encouraged to contact Applicant's undersigned attorney to resolve any remaining issues in order to expedite examination of the present application

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,



Charles A. Leyes
Registration No. 61,317

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

LEGAL02/30652649v1